クラウドサービスの安全性評価に関する検討会 中間とりまとめ（案）に対する意見

2019年4月16日

総論

BSA | Software Alliance (BSA)[1] は、「クラウドサービスの安全性評価に関する検討会中間とりまとめ（案）」（以下「中間とりまとめ」といいます。）について、総務省及び経済産業省に対して以下の通り意見を提出します。

BSA は、総務省及び経済産業省が、政府全体におけるクラウドの利用拡大及びより良いクラウドサービスの安全性評価手続の策定に全力で取り組んでおられることを高く評価します。また、中間とりまとめが、各府省情報化統括責任者（CIO）連絡会議により決定された「政府情報システムにおけるクラウドサービスの利用に関する基本方針」に掲げられた「クラウド・バイ・デフォルト原則」の重要性を認識し言及していることも、大変意義があると考えます。さらに、日本政府が、諸外国におけるクラウド導入に関する様々な実務を調査して、中間とりまとめ作成の参考にされたことを歓迎します。

BSA 会員企業は、最先端のクラウドコンピューティング技術及びサービス提供で世界を牽引しており、これを利用することによって、政府が、ネットワークセキュリティやシステムの可用性を高めながら、その俊敏性、生産性及び革新性を向上することを支援しています。

クラウドサービスプロバイダー(CSP)は、地理的な分散と規模の経済を利用して、潤沢なリソースがある企業であっても保有できないような、効率性や信頼性が高く安全なソフトウェアを介したサービスを提供するため、多くの場合、複数国の市場で同時に事業展開しています。そのため、安全で効果的なクラウドサービスの採用を促進する方針は、他国の公共セクターのクラウドの安全性評価及び認証制度と相互運用性があり、また、国際規格に適合していることが不可欠となります。

---

[1] BSA | The Software Alliance (BSA | ザ・ソフトウェア・アライアンス) は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員は世界で最もイノベーティブな企業で構成されており、経済を活性化させ、現代生活を向上させるソフトウェア・ソリューションを創造しています。ワシントン DC に本部を置き、60 カ国以上で活動する BSA は、正規ソフトウェアの使用を促進するコンプライアンス・プログラムを先導し、技術革新の推進とデジタル経済の成長を促す公共政策を提唱しています。

BSA の活動には、Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

また、公共セクターにおけるクラウド利用の安全性評価制度を考える上では、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）といった異なるクラウドコンピューティングサービスモデルについても考慮しなくてはなりません。これらのモデルは、CSP とユーザーと顧客の間の関係性、セキュリティに関する責任共有とその配分、運用効率性、クラウド環境における信頼性等を含む様々な点でそれぞれ異なっており、そのためそれぞれに適切なアプローチも異なります。そして、この責任共有は、しばしば、クラウドサービスレベルアグリーメント（クラウド SLA）に記載されています。

さらに、提案されているクラウドサービスの安全性評価の制度（以下単に「評価制度」といいます。）は、全ての政府機関において統一的にリスクベースアプローチ及び多層防御のアプローチを確実に採用し、政府機関及び今後この評価制度を取り入れる他の組織において安全かつ効果的なクラウドサービスの導入を促進するものである必要があります。

提言

上記の包括的な方針に加え、中間とりまとめの各項目について、BSA は以下の通り具体的にコメントをします。

「2.政府における情報・情報システムのクラス分けについて」及び「4.4.システム全体のアーキテクチャについて」

中間とりまとめは、情報及び情報システムのクラス分けに関する考え方を記載しており、これは、クラウドコンピューティングシステムの安全性を検討する上で重要な考慮点を示しています。クラウドサービスが発展するにつれ、クラウドアーキテクチャは革新を遂げ、異なる管理の設定を適用した別個のコンテナを使用することで、同一のクラウドアーキテクチャ内でも、異なるセキュリティ、プライバシー、機能要件に対応した安全性ルールを適用させることを可能にしました。これらの革新により、クラウドシステムにおける安全性要件を充足するソリューションの柔軟性が増し、多様性が広がりました。

クラウド安全性の政策は、これらの革新を認識し、機密情報の安全性を確保するための様々なアプローチが持つ柔軟性と多様性に適応したものであるべきです。中間とりまとめ「2.政府における情報・情報システムのクラス分けについて」及び「4.4.システム全体のアーキテクチャについて」は、機密性の高い情報を保護する方法として「システムの分離」を検討することを推奨しています。しかし、先進的なクラウドコンピューティングアーキテクチャにおいては、物理的に情報システムを分離することは、安全性の観点から不要であることが多く、却って、そのようなシステムに保存された情報へのアクセスと利用が低減し、セキュリティに関する誤解を生む等、意図しない結果をもたらす可能性があることが十分認識されるべきです。

また、政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）（以下「政府統一基準」といいます。）において、物理的なネットワークからの分離は、リアルタイムにセキュリティアップデートを受けられる利点を妨げ、却ってサイバーセキュリティリスクを増大させる可能性があるにも関わらず、セキュリティの解決策として推奨されている(政府統一基準 5.2.1(2)a 項参照)ことについて、BSA は引き続き懸念を有しています。今後、クラウドの安全性評価に関する議論を政府統一基準に反映させる際には、BSA が

以前政府統一基準に関して提出したパブリックコメント[2]を参照くださるようお願いします。この点、クラウドの安全性に関する政策は、ユーザーのセキュリティ、プライバシー及び機能要件に応じた具体的な統制目標とコンピューティング環境に基づいて、多層防御のアプローチによるサイバーセキュリティ防御を推進すべきです。

さらに、情報のクラス分けについてのアプローチは、既存のベストプラクティスと整合性を有する必要があると考えます。特に、情報の機密性のクラス分けの参考として、米国国立標準技術研究所(NIST)の Special Publication(SP)800- 60[3]及び Federal Information Processing Standard(FIPS)199[4]を使用することを BSA は推奨します。

「3.2.　制度のフレームワーク」について

BSA は、本フレームワークにおいて「既存の仕組みや認証制度等が最大限活用できるようにすること」との提案を全面的に支持します。この点に関連して、確実に、監査及び評価プロセスを十分迅速に行うことができる評価制度を日本政府が実施していただけるよう要望致します。

中間とりまとめには、「クラウドサービスの導入によるメリットを活かすためにも、システム調達全体としてクラウドサービス導入以前よりも費用が下がるよう、制度設計する必要がある」と記載されています。これは重要なポイントですが、クラウドコンピューティングソリューションを実装するためのトータルコストを従来の情報システムと比較するには、調達コストのみならず、要員、メンテナンス、構内の物理的安全確保に関する他の費用も含めて計算する必要があります。言い換えれば、トータルな運用コストについて、オンプレミスとクラウドサービスを比較することが極めて重要です。もっとも、コストがクラウドサービスを利用するかどうかを決定する唯一の要因ではないことを認識することも重要です。調達基準は、ソリューションが最終的にユーザー要件を満たすことを確実にするため、パフォーマンス、レイテンシー、潜在的なトレードオフ等の他の要因も含めることができるよう柔軟性を有するべきです。

「3.3.　制度の詳細設計」について

・民間企業の基準策定への参加

2019 年夏頃までに策定される管理基準案は、CSP にとって極めて重要です。日本政府が、管理基準及び関連する方針、ガイドライン、ルールを策定するプロセスにおいて透明性を保つとともに、プロセス全体を通じて BSA 会員企業を含む関係ステークホルダーから助言を得るよう BSA は提言します。日本政府が重大な決定をする際は、事前に CSP にフィードバックを求め、民間企業から十分な専門知識の提供を受けたうえで関連する基準や方針を策定することが不可欠です。

---

[2] BSA が提出したパブリックコメントは、https://bsa.or.jp/wp-content/uploads/bsa_20180628.pdfでご確認ください。

[3] SP 800-60 Vol. 1 Rev. 1: Guide for Mapping Types of Information and Information Systems to Security Categories https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final をご参照下さい。

[4] FIPS PUB 199: Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf をご参照下さい。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

・規範的な要件ではなく、リスクベースで結果指向の要件であること

評価制度及び関連ルールは、政府機関が、オープンなシステムを採用して、機密性の分類等に従い、暗号化、認証その他 CSP が提供する機能を使用して情報を管理することを可能にするものであるべきです。

管理基準に関しては、結果を重視したアプローチが重要です。なぜなら、基準が非常に詳細に定められている場合と比較して、CSP が新しい技術と情報セキュリティソリューションを継続的に開発し革新することを可能にするからです。規範的なセキュリティ要件はすぐに陳腐化するのみならず、セキュリティにおける最新技術の恩恵を受ける政府の能力を減退させます。従って、管理標準は、結果達成のための具体的な手順を規定するのではなく、結果を重視し、明確に定義された目的を記載すべきです。

・データ保管又は処理の物理的な場所に依存しないセキュリティ

中間とりまとめは、「クラウドサービスを運用するデータセンター等の物理的な基準も位置付けること」を提案しています。この点、グローバルに円滑なデータの越境移転を確保し最適化することが、規模の経済及びコスト上の利点、バックアップシステムの冗長性並びにグローバルなサイバーセキュリティ脅威に対応したシステムのリアルタイムアップデートといったクラウドサービスの恩恵を最大化するために不可欠なことを十分に認識し前提とすべきです。

「4.5.　政府内の体制構築・制度利用の実行性確保について」

監査主体、クラウドサービスの顧客又はユーザーとしての政府機関及び CSP の間で共有される情報には、CSP が保有する秘密情報が含まれる可能性があり、当事者間での守秘義務契約に服する場合があります。この点に関して、登録簿により公開される情報の適切な範囲について慎重に検討することが非常に重要です。

また、登録簿に多くの CSP が未だ登録されていない制度立ち上げ時期であっても、確実に、政府機関がクラウドサービスの利用を開始し又は継続できるよう、適切な移行措置を設けていただくよう要望します。

結び

BSA は、中間とりまとめに対する意見を提出する機会を感謝します。私どもは、本意見が中間とりまとめを完成させるにあたり有益であることを願っています。BSA は、評価制度の策定にあたり総務省及び経済産業省に是非協力させていただきたく存じます。また、BSA の会員企業及び他の CSP が管理基準及び関連ルールの作成に貢献し、4.1. 記載のシミュレーションにも参加することを真摯に希望します。本意見について、ご質問等ございましたらいつでもご連絡下さい。

以　上

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office